UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,753	11/21/2003	Alexander Hoffmann	16274.171	1445

22913 7590 03/31/2009
Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

EXAMINER	
NOBAHAR, ABDULHAKIM	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
03/31/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.**	**Applicant(s)**	
	10/718,753	HOFFMANN, ALEXANDER	
	Examiner	**Art Unit**	
	ABDULHAKIM NOBAHAR	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 February 2009*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10/08/2008*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 02/25/2009.

2. Claims 1-35 are pending.

3. Applicant's arguments with respect to the rejections of claims under 35 USC § 103 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration of the claims, a new ground(s) of rejection is made.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-21 and 25-36 are rejected under 35 U.S.C. 102(e) as being anticipated by Luo et al (EP 0 898 397 A2), hereinafter Luo.

Note: A copy of EP 0 898 397 A2 in a PDF format is attached to this Office Action for the applicant review.

Regarding claims 1, 13, 25 and 29, Luo discloses:

a host (see, e.g., Fig. 1, SMSC);

an interface electrically coupled to the host (see, e.g., col. 9, lines 16-28); and

A transceiver (see, e.g., [0017]) comprising:

a transmitter configured to transmit data signals (see, e.g., col. 5, lines 51-58);

a receiver configured to receive data signals (see, e.g., col. 7, lines 18-24); and a controller configured to encrypt a string and supply the encrypted string to a host to authenticate the transceiver (see, e.g., abstract; col. 6, lines 1-25; [0019]; col. 11 or [0034], lines 11-20; Fig. 2, steps 210 and 212),

authentication of the transceiver being contingent upon whether or not the transceiver has been certified by a manufacturer or supplier as meeting a specified quality standard (i.e., whether the transceiver is authentic or cloned). See [0020]; [0027], where the bank corresponds to the recited manufacturer or supplier; Fig. 2, steps 206 and 222 and col. 11 or [0034], lines 30-40, where the authenticity of the certificate is checked and if the certificate is not authentic the transceiver is rejected (the “NO” branch of the decision operation).

Regarding claims 2 and 4, Luo discloses:

The transceiver of claim 1, wherein the controller is configured to encrypt the string with a transceiver private encryption key (see, e.g., [0034], line 17, where the first decryption key is the private key).

Regarding claims 3 and 28, Luo discloses:

The transceiver of claim 1, wherein the controller is configured to use a transceiver private encryption key and a transceiver public encryption key to authenticate the transceiver (see, e.g., [0028]).

Regarding claims 5 and 6, Luo discloses that a bank issues the certificates and public encryption keys to the transceiver, and since end-to-end security is used (see [0017] and [0027]), thus the assigned encryption keys to a transceiver are encrypted by the issuer to be transmitted to the transceiver and normally the issuer uses its public key to encrypts the assigned keys. Therefore, Luo's teachings meet the limitation of these claims.

Regarding claim 7, Luo discloses:

The transceiver of claim 1, wherein the controller comprises an electrically erasable and programmable read only memory that is used to store a transceiver private encryption key and a transceiver public encryption key (see, e.g., [0017], where assigning keys to a transceiver, implies that the transceiver has a memory for holding the keys).

Regarding claim 8, Luo discloses:

The transceiver of claim 1, wherein the controller comprises a cryptography module for encrypting the string (see, e.g., col. 6, lines 3-10).

Regarding claim 9, Luo discloses:

The transceiver of claim 1, wherein the controller comprises an RSA encryption module for encrypting the string (see, e.g., [0031]).

Regarding claim 10, Luo discloses:

The transceiver of claim 1, wherein the receiver comprises a fiber optic receiver (see, e.g., [0002]).

Regarding claim 11, Luo discloses:

The transceiver of claim 1, wherein the transmitter comprises a fiber optic transmitter (see, e.g., [0002]).

Regarding claim 12, Luo discloses:

The transceiver of claim 1, wherein the transceiver comprises a small form factor pluggable transceiver (see, e.g., [0005], where SIM is a small form factor pluggable transceiver).

Regarding claim 14, Luo discloses:

The network system of claim 13, wherein the interface comprises an inter-integrated circuit bus (see, e.g., [0002], [0025] and Fig. 1, where the devices of the network are connected electrically, thus their interface component of these devices are inter-integrated circuit buses).

Regarding claim 15, Luo discloses:

The network system of claim 13, wherein the interface comprises a transceiver fault status line (see, e.g., Fig. 2, steps 206, 222 and 228, where a negative decision at these steps to the “NO” branches will lead to the failure of cryptographic operation. This indicates that the system of Luo has a mechanism for ending the communication which corresponds to the recited transceiver fault status line or disable line).

Regarding claim 16, the same rationale applied to claim 15 is applicable here.

Regarding claim 17, Luo discloses:

The network system of claim 13, wherein the interface comprises a transmit data in line TD+ and an inverted transmit data in line TD- (see, e.g., Fig. 1, where the transmission and receiving lines for communication are shown).

Regarding claim 18, Thomas discloses:

The network system of claim 13, wherein the interface comprises a received data out line and an inverted received data out line (see, e.g., Fig. 1, where the transmission and receiving lines for communication are shown).

Regarding claim 19, Luo discloses:

The network system of claim 13, wherein the interface comprises a loss of signal status line (see, e.g., [0002], the use of a feature such as (a loss of signal) status line is inherent in advance telecommunications networks).

Regarding claim 20, Luo discloses:

The network system of claim 13, wherein the host is one of a mainframe computer, a workstation, a server, and a storage device (see, e.g., [0018], Fug. 1 and [0025], where the SMSC could be facilitated by any type of computer).

Regarding claim 21, Luo discloses:

The network system of claim 13, wherein the host is one of a bridge, a router, a hub, a local area switch and a wide area switch (see, e.g., [0018], Fug. 1 and [0025], where the SMSC could be facilitated by any type of computer or a capable communication device).

Regarding claims 26 and 27, Official Notice is taken that as applicant on page 1, second paragraph, of the specification points out, it is a prior knowledge that in a fiber optic network the means for receiving data signals comprises means for converting optical serial data into electrical serial and the means for transmitting data signals comprises means that does the reverse operation.

Regarding claim 30, Luo discloses:

The method of claim 29, wherein the authentication signal comprises a certificate identification (see, e.g., [0028], where the distinguishable identity x corresponds to the recited certificate identification).

Regarding claim 31, Luo discloses:

The method of claim 29, wherein analyzing the authentication signal comprises decrypting the authentication signal using a public key of an issuing authority (see, e.g., Fig. 2, step 226, where decryption operation is performed during the authentication process of the certificate of the transceiver).

Regarding claim 32, Luo discloses:

A method for authenticating a transceiver, comprising:

installing a transceiver comprising a transceiver specific public key/private key pair, wherein the transceiver specific public key is encrypted with a private key of an issuing authority (see, e.g., Fig. 1 shows the installed components of a network; [0017] and [0027], where a bank issues the certificates and since end-to-end security is used, thus the assigned encryption keys to a transceiver are encrypted by the issuer for transmission purpose);

electrically coupling the transceiver to a host through a communication link (see, e.g., Figs. 1; [0025]);

requesting, by the host, the encrypted transceiver specific public key from the transceiver (see, e.g., Fig. 2, steps 210 and 212, where P includes the public key of the transceiver);

passing the encrypted transceiver specific public key from the transceiver to the host by way of the communication link (see, e.g., Fig. 1, depicts a communication link between the parties and the SMSC; Fig. 2, steps 212 and 220); and

decrypting the encrypted transceiver specific public key in the host using a corresponding public key of the issuing authority to obtain the transceiver specific public key (see Fig. 2, steps 220-226, where the M2 corresponding to the recited host receives P that includes M1's public key sent by the M1 and decrypts x to complete authentication process which is functionally equivalent to the recited limitation that uses the public key of the issuing authority to obtain the transceiver public key).

Regarding claim 33, the limitations recited in this claim are an authenticating procedure that is widely used in the cryptographic technology and Luo discloses these limitations through the steps 208-228 of Fig. 2.

generating an original authentication string in the host (Fig. 2, step 208, k is generated);

sending the original authentication string from the host to the transceiver (Fig. 2, step 212, P that includes k is sent to SMSC and sent to M2 at step 220);

encrypting the original authentication string in the transceiver using the transceiver specific private key (Fig. 2, step 210, k is encrypted);

passing the encrypted authentication string from the transceiver to the host (Fig. 2, step 220, k is included in P and is sent to the M2); and

decrypting the encrypted authentication string in the host using the transceiver specific public key (Fig. 2, step 224, where k is computed that corresponds to the recited decryption).

Regarding claim 34, Luo discloses:

The method of claim 33 comprising:

comparing the decrypted authentication string to the original authentication string (see

[0035]; and

selecting one of rejecting and accepting the transceiver based upon the comparison (see Fig. 2, steps 236 and 234).

Regarding claim 35, Luo discloses:

The method of claim 33, wherein the original authentication string is a random number (see, e.g., [0030]; [0034], where the session key k corresponds to the recited random number).

Regarding claim 36, Luo discloses:

The method of claim 1, wherein if the transceiver is authentic, the transceiver can not be cloned (see [0033] and [0034]; Fig. 2, steps 206 and 222, where if the comparison operation is positive then the certificate and as result the transceiver is authentic which proves that the transceiver has been certified by an authority and the transceiver is not inauthentic or cloned, i.e., it cannot be cloned).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Luo et al (EP 0 898 397 A2), hereinafter Luo, in view of the applicant admitted prior knowledge described in the background section of the specification and hereinafter referred to as APK.

Regarding claim 22, Luo discloses:

A transceiver (see, e.g., [0017]) comprising:

a transmitter configured and arranged to transmit data signals to an external device in response to commands from a host (see, e.g., Fig. 2, where M1 at step 212 sends P to SMSC in response to SMSC that at step 204 sends certificate of M2 to M1 which amounts to a command to the transmitter of M1);

a receiver configured and arranged to receive data signals from the external device and to pass corresponding data signals to the host (see, e.g., Fig. 2, where at steps 204 and 218 SMSC sends data to the M1 and M2 which corresponds to the receivers of M1 and M2 receive signal from SMSC); and

a controller in communication with the transmitter and the receiver and configured and arranged to communicate with the host to authenticate the transceiver with the host, wherein the controller stores a first unique transceiver-specific public key/private key pair for authentication (see, e.g., abstract; col. 6, lines 1-25; [0019]; col. 11 or [0034], lines 11-20; [0020]; [0027], where the bank assigns the keys to the transceivers which indicates that the transceiver has a memory to hold the keys), Luo, however, does not expressly disclose that the first unique transceiver-specific public key/private key corresponding with a manufacturer of the transceiver.

APK discloses that manufacturers and suppliers have developed strict quality standards that must be met before their fiber optic transceivers are certified (i.e., authentic not cloned) for use in systems (specification, pages 1 and 2, paragraphs 3 through 6). This indicates that that the transceiver's public key/private key pair is assigned by the manufacturer to prove the transceiver authenticity. Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to employ a manufacturer-certified transceiver as described in APK in the system of Luo in order to have a more reliable transceiver to prevent possible loss due to the failure of the transceiver (see APK, page 1, lines 20-28).

Regarding claims 23 and 24, Luo discloses:

A distinguishable identity x (corresponding to the recited access code) is assigned to each transceiver (see [0028]) that is transmitted to the other party (i.e., host) along with the public encryption key for the purpose of transceiver's certificate authentication. Since the identity x is used with the public encryption key for the same purpose and belong to the same transceiver, thus x is associated with the public encryption key. With respect to a second access code associated with a second public/private key pair, Official Notice is taken that in order to have a strong security system, it is old and well known practice in the art of cryptography to have other cryptographic keys for replacement and substitution of the keys that are currently used either when the keys are expired or if it is suspected that the keys have been used by an unauthorized entity. Therefore, the teachings of Luo meet the limitations of claims 23 and 24, i.e., the following:

wherein the first unique transceiver-specific public key/private key pair is associated with a first access code and the controller stores a second unique transceiver-specific public key/private key pair for authentication, wherein the second unique transceiver-specific public key/private key pair is associated with a second access code.

wherein the first unique transceiver-specific public key/private key pair is used for authentication in response to the host communicating the first access code to the controller and the second unique transceiver-specific public key/private key pair is used for authentication in response to the host communicating the second access code to the controller.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

March 24, 2009